Privacy and Security Solutions for Interoperable Health Information Exchange

Kentucky e-Health Privacy and Security Collaboration: Final Implementation Plan Report

Subcontract No. 25-321-0209825
RTI Project No. 9825

Prepared by:

Cabinet for Health and Family Services
University of Kentucky
University of Louisville

Submitted to:

Linda Dimitropoulos, Project Director
Privacy and Security Solutions for
Interoperable Health Information Exchange

Research Triangle Institute
P. O. Box 12194
3040 Cornwallis Road
Research Triangle Park, NC 27709-2194

April 16, 2007

Acknowledgements

The Kentucky Cabinet for Health and Family Services (CHFS) would like to acknowledge the following staff and Privacy and Security Project members for their contributions to this report:

Steering Committee/Implementation Work Group:

Chairs:

Bob Esterhay, MD, Chair, Health Management and Systems Sciences, University of Louisville School of Public Health

Carol Steltenkamp, MD, MBA, Chief Medical Information Officer, UK HealthCare, and Assistant Dean for Clinical Affairs, University of Kentucky School of Medicine

Members:

Jeanne Reiners, Corporate IT Manager, Baptist Healthcare System and the Chair of the Variations Working Group

Vickie Yates Brown, J.D., Member at Greenebaum, Doll & MacDonald and Chair of the Legal Working Group

Jeff Rose, Director of Technology Solutions at ConnectKentucky and Chair of the Solutions Working Group

Shawn Crouch, Chief Of Staff, CHFS

Trudi Matthews, Senior Policy Advisor, CHFS

Dr. Brent Wright, Program Director, U of L Family Practice Residency Program, TJ Samson Family Practice Center

Terry Jackson, Director of Information Services, Trover Foundation

Joni Lemke, Program Director, Wellpoint/Anthem Privacy and Security Office

Shannon Pratt, Government Relations Director, American Cancer Society

Marti Arvin, Privacy Officer, University of Louisville

Legal Services Contractor

Ned Benson, Attorney,
Sturgill, Turner, Barker, Moloney

The Kentucky project team consisting of staff from the Cabinet for Health and Family Services, the University of Kentucky, and the University of Louisville were responsible for compiling this report. The recommendations and findings contained in this report do not necessarily reflect the views of the project participants or their organizations.

CHFS Project Staff

Trudi Matthews, Senior Policy Advisor and Project Director
Office of the Secretary

Linda Robinson, IT Systems Consultant
Office of Information Technology

Smita Prasad, Intern
Office of Health Policy

Richard Stout, Intern
Office of Health Policy

University of Louisville Project Staff

Robert J. Esterhay, M.D., Associate Professor and Chair
Department of Health Management and Systems Sciences
School of Public Health and Information Sciences

Susan Olson-Allen, Ph.D., Project Coordinator
Department of Health Management and Systems Sciences
School of Public Health and Information Sciences

Bruce W. Edwards, B.S., Information Security Officer

Marti Arvin, J.D, Privacy Officer

University of Kentucky Project Staff

Carol Steltenkamp, MD, MBA, Chief Medical Information Officer, UK HealthCare, and Assistant Dean for Clinical Affairs, University of Kentucky School of Medicine

Julia F. Costich, J.D., Ph.D., Chair
Department of Health Services Management
College of Public Health

Carol L. Ireson, R.N., Ph.D., Associate Professor
College of Public Health

Table of Contents

I. Background

Introduction

On March 8, 2005, Governor Fletcher signed Kentucky's landmark e-Health legislation, SB2, which created the Kentucky e-Health Network Board to oversee e-Health efforts in the state. It also established the Healthcare Infrastructure Authority, a partnership of Kentucky's two major research universities – the University of Kentucky (UK) and the University of Louisville (U of L) – to provide leadership for the Board. The Cabinet for Health and Family Services (CHFS), at the urging of Governor Fletcher, took a leading role in fostering e-Health in the state by providing staff support to the Board and working with the leadership of chairs from UK and U of L to undertake several strategic initiatives in the year following SB2's passage and enactment.

One of the first projects undertaken by the e-Health Board was the **Kentucky e-Health Privacy and Security Collaboration**. In May 2006, Kentucky was one of 33 states awarded a contract to participate in the Health Information Security and Privacy Collaboration (HISPC), a federally-funded collaboration involving the Office of the National Coordinator, the Agency for Healthcare Research and Quality, RTI, and the National Governors Association. Governor Ernie Fletcher designated CHFS as the project manager but requested that CHFS staff work collaboratively with faculty from U of L and UK on the project.

The goal of the project is to assess at the state and local levels how privacy and security practices and policies affect health information exchange (HIE). Under federal contract requirements, Kentucky was responsible for organizing a large group of Kentucky stakeholders to participate in a number of Working Groups and committees with specific responsibilities for portions of the project:

- a **Steering Committee** to oversee the project and develop a plan for implementing recommendations for Kentucky
- a **Variations Working Group** to assemble organization-level business practices related to the confidential and secure exchange of health information
- a **Legal Working Group** to analyze barriers to information exchange and map those barriers back to applicable law and regulation
- A **Solutions Working Group** to develop an inventory of possible approaches to dealing with any barriers or other challenges identified.

Kentucky's e-Health Privacy and Security Collaboration Stakeholder Community consisted of more than 60 volunteers and staff from a wide variety of stakeholder organizations and backgrounds.

Each partner on the project had a specific role and set of duties. CHFS is responsible for overseeing the project and staffing the Steering Committee and the Legal Working Group. In addition, CHFS engaged a law firm to develop a compendium of state e-

Health and privacy and security laws, and assist the Legal Working Group with identifying and mapping the barriers in law and regulation related to health information exchange. The staff at the University of Louisville were responsible for the Variations Assessment process, the Variations Working Group, and preparation of the Variations Report. University of Kentucky staff were responsible for the Solutions Analysis and the Solutions Working Group. The Steering Committee co-chairs, Drs. Robert Esterhay (UofL) and Carol Steltenkamp (UK), served as overall coordinators for the staff of their respective universities that are involved in the project and their university's deliverables.

Purpose and Scope of Report

Establishing an efficient and effective interoperable health information exchange in Kentucky is of top priority, and Kentucky stakeholders on the Kentucky e-Health Network Board and its various groups and committees are working diligently to confront the barriers to adopting health information technology. Ensuring the privacy and security of protected health information in an electronic environment is critical to creating public trust and support for e-Health, ensuring providers have access to information without increasing their risk of lawsuits or data breaches, and achieving the efficiencies necessary to improve care and affordability.

The main objective of this report is to outline the approaches and functional steps that Kentucky's Privacy and Security Collaboration can take to address the privacy and security issues that were identified during the variations and solutions process and that may affect and impede health information exchange in Kentucky. The variations, barriers, and solutions utilized in this report were identified by the Kentucky e-Health Privacy and Security Collaboration project team consisting of staff from the Cabinet for Health and Family Services, the University of Kentucky, and the University of Louisville as well as a multitude of stakeholders from across Kentucky that served on the Steering Committee and Working Groups for the Project.

The findings and recommendations from the Kentucky e-Health Privacy and Security Collaboration will be forwarded to the Kentucky e-Health Network Board and considered at its April 17th, 2007, meeting. At that meeting the e-Health Board will also seat a new Privacy and Security Committee that will be responsible for carrying out the findings and recommendations from this Implementation Plan and the Final Variations and Solutions Report.

Assumptions and Limitations of this Report

This report stems from a federally funded project that used specific research design and data collection methods to ensure a coordinated schedule and a uniform process across all states participating. At the center of the study was the use of 18 health information exchange scenarios. All stakeholders involved in the project in Kentucky were asked to utilize these scenarios during the Assessment of Variations and Solutions process.

The findings of this project, while broad in scope, are not intended to be an all-exhaustive list of every e-Health and privacy and security issue in Kentucky. Many more issues and solutions could be developed related to health information exchange and privacy and security than what is contained in this report. This Implementation Plan is not intended to be an overarching action strategy for developing a statewide e-Health network. The overarching mission and vision for e-Health in Kentucky is provided in the Kentucky e-Health Annual Report (released January 2007) and e-Health Action Plan (forthcoming). Thus, the scope of this Implementation Plan is more narrowly focused on the business practices, legal barriers and other issues related to health information privacy and security and how Kentucky proposes to address the challenges and concerns identified through this project.

II. Summary of Key Challenges and Analysis of Solutions

Variations Assessment and Legal Mapping Findings

For technology to improve the efficiency and quality of health services to the greatest degree possible, health information exchange must be largely instantaneous and automatic. This ability is facilitated largely by the use of a set of recognized rules or standards among organizations, including standards for protecting the privacy and security of the information. Kentucky's e-Health Privacy and Security Collaboration produced a number of important findings and recommendations regarding the challenges related to various health information exchange situations, including the following:

- **Widespread misunderstanding and confusion concerning state and federal laws relating to the privacy and security of health information**

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) provided baseline protections for health information across the United States, but other state and federal laws also contain provisions regarding the privacy and security of protected health information (PHI). Project participants expressed great concern regarding the large number of differing standards and interpretations between state and federal laws protecting health information. Multiple state or federal laws and regulations that deviate significantly from the baseline privacy and security protections that HIPAA provides can be particularly problematic in an electronic information environment.

Health care providers and practitioners in particular expressed a great deal of uncertainty about when patient data may be released and to whom. Issues arose regarding the release of information to payers for administrative purposes as well as for organizations to monitor patient management. Release of information for non-medical purposes, such as to police, parents of adult children, employers, marketers and government agencies were also particularly problematic.

- **Issues related to handling of sensitive protected health information**

Particularly sensitive areas of protected health information include information related to mental health, substance abuse, HIV/AIDS, sexually transmitted diseases and some other communicable diseases. These types of sensitive conditions are afforded special protections due to the stigma and potential negative consequences of inappropriate information disclosure. While agreeing that special protections for sensitive health information are important, project stakeholders also noted the difficulty of ensuring compliance with all the provisions found throughout state and federal law related to sensitive PHI. The differing provisions and standards for appropriate disclosure means that, when in doubt, health organizations do not share any health information. However, this policy could affect greatly both the continuity of care and the quality of care provided as electronic health information exchange becomes customary. Some

participants urged the development of a more coherent set of standards around sensitive PHI. Such standards could have two positive benefits: 1) ensuring to a greater degree that sensitive PHI is afforded the special protection it deserves and 2) making it easier for health organizations to comply with the law.

- **Technology limitations related to electronic information exchange**

The project examined many limitations to currently available health information technology. Identity management is an issue for any technology application, but it is especially important with health information where life and death matters are at stake. Determining policies and practices for appropriate access, authentication, authorization, and auditing for information systems are critical to protecting the privacy and security of electronic health information. In addition, interoperability is a critical issue to health information exchange because health information systems currently cannot easily communicate with one another. The lack of a standard way to match patient records across health organizations is another technology challenge. Finally, there are associated problems with the various types of data transfer and ensuring secure transmission.

- **Relative silence in law on health information exchange**

Much of Kentucky law and regulation governing health care and public health assumes and reinforces a paper-based environment rather than an electronic environment for health information management. Emerging practices such as e-prescribing, health information exchange, RHIOs, and personal health records are so new and dynamic that clear legal parameters do not exist yet. Without clear policy guidance, health organizations may be reluctant to move aggressively into the world of e-Health. In some cases, law and regulation may simply be out-dated and have not changed in decades to reflect current practices. The process of updating privacy and security statutes and regulations is difficult because these statutes and regulations are scattered throughout state codes.

- **Concern regarding business risk and adverse legal action if information exchanged**

The ambiguities between state and federal law, the current limitations to technology and the “newness” of e-Health mean that there are inherent risks to early adopters of health information technology and exchange. While many providers, administrators and practitioners have managed to deal with these challenges, there is an underlying concern that a specific situation may uncover hidden problems, thus exposing health care entities to unanticipated risk to both their business reputations and to adverse legal action.

Analysis of Solutions

The task of the Solutions Working Group was to review the business practices that were identified by the Variations and Legal Working Groups as barriers to health information exchange.

Initially project staff and the Solutions Working Group focused their attention on the barriers that could be mapped back to Kentucky state law or regulation. The group believed that issues with Kentucky laws, regulations, or practice should be the major focus for the Solutions Working Group to examine and develop clear recommendations. Nevertheless, many business practices that affect health information exchange were not driven by legal but technological and organizational barriers. Thus, the Solutions Working Group and staff also needed to identify solutions to these types of barriers. Finally, many practices identified as barriers were based on common misinterpretations related to privacy and security law and practice and therefore require solutions aimed at education and awareness to address.

The group's focus on Kentucky laws, regulations and practices is intended to remedy inconsistency and contradiction found among those laws, regulations and practices rather than creating new legislation. The consensus among the Solutions Working Group was that providing clear, consistent rules on how to protect and secure health information and when exchange of health information is appropriate and allowed would remove or mitigate many of the barriers identified by the Variations and Legal Working Groups.

Overall, in examining the business practices classified as barriers, the project staff and Solutions Working Group members were able to identify five basic categories of action that Kentucky could take to deal with the identified barriers. The following categories of action defined in the final report address:

Statutory Action: The solutions in this category involve reviewing, revising, or amending state or federal laws that affect the exchange of health information, the privacy and security of health information, and the related healthcare diagnosis and treatment activity. The solutions in this category address a number of barriers to health information exchange (HIE) identified during this project including :

- Inconsistent federal law
- Inconsistent state law
- Misinterpretation or understanding of HIPAA law.

Regulatory Action: The solutions in this category identify areas where existing rules and regulations may be relaxed, modified, expanded, or better explained to facilitate HIE without the need for legislative action. These solutions address the following barriers to HIE:

- Differences in state and federal regulation
- Lack of clarity regarding state and federal regulation
- Fear of violating a regulation and subsequent sanctions or litigation.

Administrative/Organizational Action: The solutions in this category address the need to amend, create, and standardize administrative actions, business policies and practices utilized by health care providers at the individual and institutional level resulting from the following barriers:

- Longstanding cultural trends and norms within an organization
- Differences in organizational policies and practices.

Technological Solutions: The solutions in this category identify ways in which technology can be used as a solution to the barriers posed by HIE. How can health information technology improve the secure transmission of health information? What technological tools, skills or training may address the barriers to HIE? These solutions target the following barriers:

- Complexity of digital or electronic communication
- Insufficient use of electronic health information.

Public Awareness and Education: The solutions in this category address the need for increased public awareness through training and education of consumers, health care providers, government officials, professional associations, employers, public officials, researchers, and educators about the rules governing HIE, the benefits to electronic HIE, and their respective rights and obligations regarding enhanced quality of care. These solutions address the barrier of:

- Limited or lack of education about HIE and privacy and security laws
- Provider concern about business reputation and public relations issues.

III. Review of State Implementation Planning Process

To assist with Kentucky's Privacy and Security Collaboration, the Cabinet and the two universities worked with the project's Stakeholder Community, a group of more than 60 volunteers from a wide variety of stakeholder organizations throughout Kentucky. Because Kentucky is a smaller state, Kentucky's HISPC project proposal merged the Implementation Plan Working Group with the Steering Committee. Thus, the Steering Committee members have directed their work to the eventual development of an Implementation Plan. The Privacy and Security Steering Committee has also served as the overall advisory group for the project. The Steering Committee consists of 12 members, two of whom chair the Committee and come from U of L and UK. Additional members of the Steering Committee are the three working group chairs for the project as well as a physician, a health plan, a hospital, a state government, and a privacy and security expert, as well as a consumer representative.

The HISPC Steering Committee has met once a month on the second Wednesday of the month since July of 2006. The Steering Committee has been apprised of the progress of the project, reviewed and submitted comments on all reports and deliverables, and provided guidance to project staff. In addition, Kentucky's project proposal outlined that upon completion of the HISPC project the findings from the project would be given to a permanent committee of the Kentucky e-Health Network Board for action and implementation. CHFS staff have updated the KEHN Board on the progress of the project with the goal of having the HISPC project integrate eventually into the regular work of the e-Health Board. On January 18, 2006, during its regular meeting, the Kentucky e-Health Network Board approved a proposal to seat a permanent Privacy and Security Committee. A slate of candidates will be appointed at the April 2007 e-Health Board meeting.

After submitting the Interim Solutions Report in January 2007, project staff convened a stakeholder feedback session during Kentucky's e-Health Summit on January 19, 2007. A group of about 20 participants from a variety of areas were asked to review the two Interim Draft Reports, provide feedback on the overall findings and work of the project, and to make recommendations on how to move forward with the Implementation Plan. Though some of the participants in this session had participated in the project at some point, for others this was their first opportunity to review the reports. Several participants expressed concern that the reports were too technical and recommended that project staff move away from RTI's recommended format and structure to make them more user-friendly for individuals who were not familiar with the project, especially for those who were not privacy and security experts.

For the final phase of the project, the Steering Committee met every two weeks via conference call to review and complete work on the final reports and implementation plan for this project. The Steering Committee discussed in greater detail the outstanding issues with the project, how the project would move forward with implementation after

federal funding and technical assistance was completed, and how to make project findings useful for Kentucky stakeholders.

The Steering Committee also recognized how critical an actionable plan was for the ongoing work of the Kentucky e-Health Network Board. To that end, the Steering Committee recommended that the Privacy and Security Committee's first responsibility be to address the findings from the Kentucky e-Health Privacy and Security project and the recommendations in the Implementation Plan. The Privacy and Security Committee will be appointed at the April 2007 e-Health Board meeting and will begin work shortly thereafter. Many volunteers who served on the Steering Committee and other working groups have agreed to serve on the Privacy and Security Committee to ensure continuity and implementation of the project's findings. In addition, Kentucky's forthcoming e-Health Action Plan, which will guide Kentucky's e-Health efforts over the next five years, has incorporated the work of this project into Kentucky's long-term planning for e-Health.

IV. State Level Implementation Plans

As discussed above, the most significant portion of Kentucky's Implementation Plan will be formation of a permanent Privacy and Security Committee of the KEHN Board. This committee is slated to be seated in April 2007 following the completion of Kentucky's Privacy and Security Project. The committee's charge will include further analysis of the findings and implementation of the final recommendations from the Kentucky Privacy and Security Project. Members of the HISPC project will be given the opportunity to serve on the committee with final approval by the board chairs, helping to ensure continuity between the Project and the work of the committee. The e-Health Network Board approved appointing this committee at its January 2007 meeting. This important synergy allows for coordinated statewide effort surrounding the privacy and security of health information to feed directly into ongoing e-Health efforts in Kentucky, ensuring the sustainability of this project's outcomes and long term impact. A presentation summarizing the HISPC project is also planned for the e-Health Board at its April 2007 meeting.

The first responsibility of the Privacy and Security Committee will be to address the solution categories outlined in the Final Report and the Implementation Plan. For most activities the Kentucky e-Health Network Board generally will oversee implementation with the Privacy and Security Committee specifically charged with working on the activities. Unless indicated otherwise, the Privacy and Security Committee will own the Implementation Plan activities and will be responsible for tracking and reporting on progress against the plan to the KeHN Board with a focus on key milestones for currently funded activities. The timelines and milestones for many of the activities that require legislative action are driven by the legislative calendar. Some of the activities do not have current funding identified. Those activities may not have a timeline or milestone associated with them as additional funding sources will need to be identified before they can be implemented by the e-Health Board. The implementation plans for

the five categories of Solutions included in the Solutions Report are provided in the following tables.

State-Level Implementation Plans

Category 1: Statutory Action			
Goal: Consistent state laws that allow confidential and secure electronic health information exchange.			
Outcome Objective: Kentucky's health care community has clear legal standards for the exchange of protected health information electronically.			
Outcome Measure: Statutes identified in the legal analysis are revised, consolidated or created to facilitate the electronic exchange of health information.			
Activities	**Owner** **Stakeholders** **Resources Required**	**Priority** **Timeline** **Milestone**	**Funding**
5.1.1 Review, and where necessary, revise definitions related to health information sharing and exchange that presently exist in statute to make them consistent with the present meaning in a paper and electronic environment.	Owner: Privacy and Security Committee	Priority: Urgent	Current CHFS e-Health Funding
	Stakeholders: All providers, payors, practitioners and purchasers	Timeline: 2007 – 2008	
	Resources Required: CHFS Staff	Milestone: Legislation prepared by October 2007 for stakeholder input, for 2008 legislative session.	
5.1.2 Recommend ways to reconcile differences between state and federal laws relating to preemption and interpretation, including identification and management of sensitive health information.	Owner: Privacy and Security Committee	Priority: High	Additional External Funding Needed
	Stakeholders: All	Timeline: December 2008	
	Resources Required: CHFS Staff, Legal Services	Milestone: Publication, Internet Resources	
5.1.3 Consider consolidating or referencing statutes related to the exchange of health information to resolve conflicts among Kentucky laws and between Kentucky laws and HIPAA.	Owner: Privacy and Security Committee	Priority: Low	Current CHFS e-Health Funding
	Stakeholders: Health care providers	Timeline: Unknown	
	Resources Required: CHFS Staff	Milestone: Analysis of this option completed by Privacy and Security Committee	

Category 2: Regulatory Action			
Goal: Consistent rules and regulations to facilitate private and secure exchange of electronic health information.			
Outcome Objective: Kentucky's health care community adheres to uniform operational standards for exchanging health information.			
Outcome Measure: Regulations related to medical record keeping revised to create uniform standards for health information exchange across health care entities.			
Activities	**Owner** **Stakeholders** **Resources Required**	**Priority** **Timeline** **Milestone**	**Funding**
5.2.1 Establish the Privacy and Security Committee of the Kentucky e-Health Network Board and charge it with providing clarification on existing regulations and creating regulations that will advance HIE.	Owner: Kentucky e-Health Network Board	Priority: Urgent	Current CHFS e-Health Funding
	Stakeholders: All especially health care providers	Timeline: April 2007	
	Resources Required: CHFS Staff	Milestone: Privacy and Security Committee appointed.	
5.2.2 Develop a policy framework for consistent identity verification and management system of providers and patients that request and transmit PHI.	Owner: Kentucky e-Health Network Board	Priority: High	Additional External Funding Needed
	Stakeholders: Health care providers, practitioners, RHIOs/HIEs	Timeline: Unknown	
	Resources Required: KY RHIOs, CHFS Staff, Stakeholders	Milestone: Publication, Internet Resources	
5.2.3 Develop policies that address sharing of patient health information among private and public sector providers within and among states during an emergency.	Owner: Privacy and Security Committee	Priority: High	Additional External Funding Needed
	Stakeholders: Health care providers	Timeline: Unknown	
	Resources Required: CHFS Public Health Staff, Local Health Depts., Homeland Security	Milestone: New regulations	
5.2.4 Establish an interstate task force to develop HIE policies for the exchange of information between states.	Owner: Privacy and Security Committee	Priority: Low	Additional External Funding Needed
	Stakeholders: All	Timeline: Unknown	
	Resources Required: Other State Agencies, CHFS Staff	Milestone: Task force developed	

Category 3: Administrative/Organizational Action			
Goal: Adoption of administrative procedures, business policies and practices utilized by health care providers at the individual and institutional level to protect privacy and security			
Outcome Objective: Kentucky's health care, public health and business communities work together to create and maintain financially sustainable and efficient health information exchanges at the local and state level.			
Outcome Measure: Protecting and securing health information does not present a barrier to the formation of HIEs and business development as demonstrated by a revenue flow capable of sustaining the organization			
Activities	**Owner** **Stakeholders** **Resources Required**	**Priority** **Timeline** **Milestone**	**Funding**
5.3.1 Produce and distribute checklists, inventories of successful practices, templates, and other resources required for the establishment of a secure HIE system.	Owner: Privacy and Security Committee	Priority: High	Additional External Funding Needed
	Stakeholders: All	Timeline: Unknown	
	Resources Required: CHFS Staff	Milestone: Publication, Internet Resources	
5.3.2 Provide technical support for RHIO/HIE initiatives to identify financial resources and develop sustainable business models.	Owner: Health Information Exchange Committee	Priority: High	Additional External Funding Needed
	Stakeholders: All	Timeline: 2008	
	Resources Required:	Milestone: Publication, Internet Resources, Grant funding or Personnel	

Category 4: Technological Solutions			
Goal: Adopt a secure technological framework.			
Outcome Objective: Kentucky's health care providers have access to a secure statewide health information network to ensure health information is shared in a private/secure environment.			
Outcome Measure: Protecting and securing health information does not present a barrier to providers investing in HIT and/or HIE systems			
Activities	**Owner** **Stakeholders** **Resources Required**	**Priority** **Timeline** **Milestone**	**Funding**
5.4.1 Convene a second Kentucky e-Health Summit to share technological methodologies that will address the barriers to HIE.	Owner: Kentucky e-Health Network Board	Priority: Urgent	Registration Fees, Private Sponsors
	Stakeholders: All	Timeline: December 2007	
	Resources Required: CHFS Staff	Milestone: Summit held with sessions related to technology challenges related to privacy and security	
5.4.2 Facilitate the development of a statewide electronic health network.	Owner: Kentucky e-Health Network Board	Priority: High	Additional External Funding Needed
	Stakeholders: Health care providers, plans and third-party payors, state government	Timeline: 2005 – 2011	
	Resources Required: KY RHIOs, CHFS Staff	Milestone:	
5.4.3 Utilize the expertise of the Privacy and Security Committee members to develop and advise on best-in-class security and privacy solutions and technologies, such as the use of digital signatures, automated proactive audit mechanisms, and identity management for use in the HIE environment.	Owner: Privacy and Security Committee	Priority: Urgent	Current CHFS e-Health Funding
	Stakeholders: All including IT vendors, CIOs, and privacy and security officers	Timeline: 2008	
	Resources Required: CHFS Staff	Milestone: Publication, Internet Resources	
5.4.4 Use financial incentives and other means to encourage providers to invest in HIT and implementation of private and secure HIE methodologies and systems.	Owner: Kentucky e-Health Network Board	Priority: Moderate	Additional External Funding Needed
	Stakeholders: All	Timeline: 2008	
	Resources Required: CHFS	Milestone: Funding secured and funding distribution method determined.	

Category 5: Public Awareness And Education			
Goal: Raise Community Awareness.			
Outcome Objective: The health care community and general public is aware and understands the importance of the health information technology activities taking place at the nation, state, and local levels.			
Outcome Measure: Percent of general public aware of health information exchange, based on a polled sample of Kentucky's population.			
Activities	**Owner** **Stakeholders** **Resources Required**	**Priority** **Timeline** **Milestone**	**Funding**
5.5.1 Prepare and distribute information resources that clarify and address the inconsistent interpretation of relevant state law and HIPAA, including the definition of health information exchange related terms in the paper or electronic environment, to educate healthcare providers.	Owner: Privacy and Security Committee	Priority: Urgent	Additional External Funding Needed
	Stakeholders: All	Timeline: December 2007	
	Resources Required: CHFS Staff	Milestone: Publication, Internet Resources	
5.5.2 Educate patients and consumers on methods to access and manage their health information.	Owner: Privacy and Security Committee	Priority: High	Current CHFS e-Health Funding
	Stakeholders: Health care providers and patients	Timeline: Spring 2008	
	Resources Required: CHFS Staff	Milestone: Initial education completed, plan for on-going education completed.	
5.5.3 Develop and implement public awareness and educational activities that provide accurate information in language accessible to the non-specialist, i.e. layman's terms, about electronic health records, rules governing disclosure of patient data, risks associated with paper charts, and the positive aspects of electronic health information.	Owner: Privacy and Security Committee	Priority: Moderate	Additional External Funding Needed
	Stakeholders: All, including the general public	Timeline: unknown	
	Resources Required: CHFS Staff	Milestone: Publication, Internet Resources, Educational Activities	

5.5.4 Inform stakeholders (possibly as part of Second Annual eHealth Summit) of national, state and local activities in the area of HIT and HIE	Owner: Kentucky e-Health Network Board	Priority: High	Registration Fees, Private Sponsors
	Stakeholders: All	Timeline: December 2007	
	Resource Requirements: CHFS Staff	Milestone: Information provided as part of the summit.	
5.5.5 Encourage the use of existing mechanisms for authorizing family members' and others' access to another's PHI, such as the durable power of attorney, health care surrogate, and living wills. Ensure that these documents authorize access to PHI in keeping with patient wishes. Identify any gaps in existing state law regarding personal representatives and others who navigate the health care system on behalf of others.	Owner: Privacy and Security Committee	Priority: Moderate	Additional External Funding Needed
	Stakeholders: Health care providers	Timeline: unknown	
	Resources Required: CHFS Staff	Milestone: Revised law and regulation	
5.5.6 Integrate and link state e-Health information with existing web sites to provide updates on state e-Health activities.	Owner: CHFS	Priority: High	Current CHFS e-Health Funding
	Stakeholders: All	Timeline: September 2007	
	Resources Required:	Milestone: Web site changes completed.	

V. Conclusion

This Implementation Plan provides an outline of the ways that Kentucky can ensure that the findings and recommendations from Kentucky's e-Health Privacy and Security Collaboration are implemented. The Kentucky e-Health Network Board and the Privacy and Security Committee will spearhead efforts to address barriers to health information exchange in Kentucky. This Implementation Plan will serve as a map of the priority items for the Privacy and Security Committee of the Board to take action on both the Kentucky-specific recommendations as well as the national-level recommendations.